Strategy Research Project

INTELLIGENCE AND INFORMATION: THE PROLIFERATION OF UNCERTAINTY

BY

LIEUTENANT COLONEL RICKY EMERSON
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
25-03-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Intelligence and Information: The Proliferation of Uncertainty

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Ricky Emerson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Diane Vanderpot
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Recently, the Intelligence Community received scrutiny for the Fort Hood shootings, the foiled Christmas day terrorist plot and the death of seven CIA operatives in Afghanistan. Following these events, policy makers examined security measures and the role of intelligence in failing to "connect the dots." This report illustrates how multiple instruments of national power and interagency cooperation enhance intelligence analysts' ability to "connect the dots." Intelligence officials must balance demands for national intelligence systems to collect more data while ensuring the most relevant information is processed and analyzed for intelligence production. Policy decisions may impact intelligence analytical priorities; adding to an uncertain threat environment. Managing uncertainty requires policies, enduring solutions that combine technology and creative intelligence analysis to facilitate capabilities growth. Solutions outlined in this report are better interoperability of intelligence and interagency databases and implementation of a national level biometrics program.

15. SUBJECT TERMS

Biometric Enabled Intelligence, Relevant Intelligence, Strategic Surprise

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC STRATEGY RESEARCH PROJECT

INTELLIGENCE AND INFORMATION: THE PROLIFERATION OF UNCERTAINTY

by

Lieutenant Colonel Ricky Emerson
United States Army

Colonel Diane Vanderpot
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Ricky Emerson

TITLE: Intelligence and Information: The Proliferation of Uncertainty

FORMAT: Strategy Research Project

DATE: 25 March 2010 WORD COUNT: 6,687 PAGES: 32

KEY TERMS: Biometric Enabled Intelligence, Relevant Intelligence, Strategic Surprise

CLASSIFICATION: Unclassified

Recently, the Intelligence Community received scrutiny for the Fort Hood shootings, the foiled Christmas day terrorist plot and the death of seven CIA operatives in Afghanistan. Following these events, policy makers examined security measures and the role of intelligence in failing to "connect the dots." This report illustrates how multiple instruments of national power and interagency cooperation enhance intelligence analysts' ability to "connect the dots." Intelligence officials must balance demands for national intelligence systems to collect more data while ensuring the most relevant information is processed and analyzed for intelligence production. Policy decisions may impact intelligence analytical priorities; adding to an uncertain threat environment. Managing uncertainty requires policies, enduring solutions that combine technology and creative intelligence analysis to facilitate capabilities growth. Solutions outlined in this report are better interoperability of intelligence and interagency databases and implementation of a national level biometrics program.

INTELLIGENCE AND INFORMATION: THE PROLIFERATION OF UNCERTAINTY

How does the Intelligence Community (IC) manage the uncertainty generated by the proliferation of information? "Intelligence failure" and "we didn't connect the dots" are sound bites painfully familiar to the IC and are indicative of a complex and uncertain security environment. These sound bites resonated throughout the news channels in the aftermath of national security incidents like 9-11, the Fort Hood shootings, the failed Christmas day 2009 terrorist incident on Flight 253 and the death of seven CIA operatives in Afghanistan. Each event highlights current security measures, intelligence analytical practices, the difficulty in collecting intelligence against asymmetrical threats and the role of decision makers and policies in determining intelligence priorities. Intelligence officials must balance demands for national intelligence systems to collect more data while ensuring the most relevant information is processed and analyzed for intelligence production. Policy decisions impact intelligence analytical priorities and add to an uncertain threat environment. Improving security and diminishing uncertainty require policies for better interoperability of national intelligence and interagency databases such as DHS, FBI and the State Department. Further, we must leverage enabling technology such as Biometrics through the implementation of a national level biometrics program.

How do these recent events impact the current national intelligence process? One obvious impact is the vast amounts of available information. As information becomes more decentralized, the ability to control and verify information becomes more challenging.[1] A fluid information environment will require a paradigm shift in how the IC gathers information for the production of relevant intelligence. Nationally, the IC must

find ways to better exploit the proliferation of information available through open source information systems. The use of information to develop intelligence entails gathering and fusing unclassified information to derive intelligence. Intelligence derived through this method is known as open source intelligence (OSINT). Intelligence collection refers to the traditional gathering of intelligence using predominantly classified sources and methods from the core traditional intelligence disciplines; Signals Intelligence (SIGINT), Human Intelligence (HUMINT) and Imagery Intelligence (IMINT).

Within DoD, the shift in the Afghanistan theater intelligence strategy calls for greater leveraging of OSINT. The new strategy calls for analysts to work with information gatherers such as engagement teams and civil affairs officers to better understand the operational environment and integrate information gathered to produce more relevant intelligence. [2]

At the national and theater levels, the respective policy makers and commanders influence information requirements. The production of relevant intelligence requires a common picture of the operational environment by both the decision maker and the analyst. Given these facts, this paper argues that recent events, specifically the near fatal bombing of Flight 253 were not IC exclusive failures but failures of multiple policy and interagency practices. In the aftermath of the Christmas Day terrorist incident, President Obama called the failed attack “a systemic failure across organizations and agencies”.[3] These agencies include not only DoD but also the State Department, CIA, FBI and organizations within the Department of Homeland Security (DHS) such as the Transportation Security Administration (TSA). Each of these agencies have different intelligence priorities, budgetary constraints and personnel issues. Further complicating

the problem are a myriad of incompatible databases that are an impediment to cross agency interoperability and effective coordination. Going forward, policy decisions within multiple agencies could impact the overall collection environment. Coordinated decisions are essential to improving intelligence interoperability and enhancing U.S. security infrastructure. Some of the potential key decisions are TSA's prioritization of and budgeting for security, policy changes enacting different screening criteria that may infringe on an individual's privacy, DHS's implementation of new watch listing procedures and a State Department review of visa requirements for entering the U.S.

Recent events highlight three familiar IC challenges regarding policies and practices that preceded and still continue post 9-11. The challenges are how to penetrate terrorist networks to collect actionable intelligence, how to balance competing current strategic priorities with more long term strategic intelligence and warning needs and how to retain the core competencies of various collection agencies while overcoming bureaucratic cultures that impede good collaboration. [4]

In the National Intelligence Strategy (NIS), the Director of National Intelligence, Dennis Blair outlined six critical mission objectives to better enable the IC to synchronize its efforts and ultimately "connect the dots". This paper will focus towards three of the six 2009 NIS mission objectives; combating extremism, provide strategic intelligence and warning and better integration of counterintelligence. [5] This paper will emphasize how a combined analytical focus weighed towards these three objectives can strengthen our ability to protect the U.S. against future threats. Further, these three NIS priorities have implications at both the national and theater level and IC analytical emphasis towards them are critical to a layered security approach.

Effective intelligence integration for execution of domestic security requires emerging means such as Biometric Enabled Intelligence (BEI) to better link foreign and domestic intelligence. BEI is also classified as Identity Intelligence (I2); information derived from an individual's distinct physical or behavioral data that is analyzed with other elements of intelligence to attain the identity of an adversary.[6] Obviously, there are other intelligence collection means that are critical and relevant to the current threat environment. BEI is an enabling technology that is tailorable towards emerging technologies and databases and its employment denies anonymity to a "shadow" threat.

To date, methods such as biometrics have been controversial with civil libertarians. However, in the aftermath of 9-11, U.S. citizens were willing to accept greater scrutiny at the payoff of increased security. In the aftermath of the Christmas day incident and Fort Hood, a window of opportunity exists for policy makers to effect a shift towards enhanced security through the use of new tools for intelligence collection. The value added for the IC is an increased ability to make progress in the handling and sharing of intelligence at local and federal levels.

Since 9/11 there have been 28 foiled terrorist plots against the U.S. of which 26 were thwarted by intelligence; the other two; Richard Reid and Abdulmutullab were stopped by passengers.[7] In short, 93% is not good enough when lives are at stake. This paper emphasizes that the threshold of 100% success and total elimination of surprise is not a realistic objective against asymmetrical threats such as extremism or other non-state actors who are not constrained by international laws or norms. However, we must continue to strive to get better.

Who's got the Smoking Dot?

The recent White House findings of the thwarted attack on Flight 253; principally faults the IC for its failure to preemptively identify the threat. The findings correctly indicate that sufficient information was available to prevent the attack. The findings noted that unlike 9-11, barriers to information sharing such as bureaucratic behavior and a component responsible for fusing the intelligence were not the cause of the failure to "connect the dots."[8] We will always have sufficient information to prevent attacks. In fact, studies of "intelligence failures" that spanned several decades indicated that problems stemmed not from collection but how the information was "collated, interpreted and communicated."[9]

In retrospect, one understands how dots should have been connected. Former CIA Chief, General Michael Hayden acknowledged challenges of sifting through vast amounts of information. "Given the vast ocean of dots that analysts have to work with prospect, this is a very daunting task every day, and for the most part they get it right. Here they didn't. They didn't connect the dots, or at least didn't connect them in time to take action."[10]

In today's security environment, the IC, specifically intelligence analysis, is still on the frontline defending U.S. security. However, security and even the collection and processing of critical information for the production of intelligence are not solely the IC's responsibility. Multiple agencies have key information or a "dot" that could be the key nugget that connects a potential plot. In most cases, the agencies do not understand the importance of the information they possess or the information does not rise to their required internal thresholds to elevate its importance. In fact, five commonalities between 9-11, Fort Hood and the Flight 253 exist; they are: 1) information overload; 2)

varying interagency priorities; 3) analytical priorities; 4) security criteria and 5) privacy. Flight 253 provides the most comprehensive illustration of each commonality. It is a recent national security incident that is relevant to the uncertainty and complexity of the current security environment and allows for a comprehensive analysis of the way ahead towards improving intelligence and its support to national security. Therefore, it will be the primary case study from which each of the commonalities is examined.

Information Overload. Post 9-11, we live in an era of increased uncertainty. The assumption is that more information will help reduce the fog of uncertainty. Instead, we have increased fog due to vast amounts of information and the various disparities across the agencies and within DoD in the analytical priorities and data processing methods. The focus is on collecting greater quantities of intelligence which generates more work on the analytical effort to sort through massive amounts of data. In effect, there is a strategy to resource mismatch. This mismatch highlights the struggle to constantly reassess priorities and match the organization of intelligence to the current collection environment.[11] In Afghanistan, the amount of collected drone video for 2010 is projected to exceed 2009 output. If continuously viewed, it is estimated that there is over 24 years of archived video footage collected in Afghanistan and Iraq from 2007 to present.[12] The effect of this collection is a backlog of vast amounts of video footage without sufficient analytical resources to exploit it. Processing information requires triage procedures to streamline collected information to ensure the most relevant information is analyzed for its intelligence value. The criteria for triaging information is a combination of the processing and analysis of the necessary information required for key decisions, the analytical resources available and the time required.

The drone collection also highlights similar challenges in the analysis of OSINT. Effective OSINT collection is critical in a counterinsurgency (COIN) environment. The vast quantities of collected OSINT data must be analyzed and assessed for validity. Strategic intelligence professionals, while utilizing OSINT; must resist the tendency to fall into a current intelligence paradigm stemming from instantaneous information availability. There must exist a balance between current intelligence and long term analysis.

Varying Interagency Criteria. Varying interagency priorities lead to internal collection and analytical efforts that are not always compatible with other organizations. The Director of National Intelligence tasked its National Counterterrorism Center (NCTC), created by the Intelligence Reform and Terrorism Prevention Act (IRPTA) of 2004, to fuse and assess all source intelligence pertaining to terrorism and counterterrorism.[13] The CIA has the responsibility to "correlate and evaluate intelligence related to national security and provide appropriate dissemination of such intelligence."[14] For example, leading up to the Christmas day 2009 incident on Flight 253, both the CIA and the NCTC had pieces of threat information regarding a potential attack. There was information about a Nigerian national, Umar Farouk Abdulmutallab, who had extremist ties with Al Qaida in the Arabian Peninsula (AQAP), a Yemen based extremist organization. The State Department knew Abdulmutallab's father had reported his son missing to American Embassy personnel in Abuja, Nigeria. The father was concerned about his son's radical religious views and his plans to travel to Yemen. There were also reports of AQAP attack plans using a Nigerian.[15]

Similar to 9-11, the Christmas day incident included fragmented information embedded within large quantities of other data. Although the missions of the NCTC and CIA are intentionally meant to provide redundancy, the dots still were not connected for a myriad of reasons. Looking at the Christmas day incident, the operational procedures of multiple agencies contributed to the fog. One prominent area is watch listing. The NCTC manages the Terrorist Identities Datamart Environment (TIDE) database which serves as the central repository for information on known and suspected international terrorist. This information is accessible by the FBI for its Terrorist Screening Center (TSC) which reviews nominations for inclusion in its master watch list, the Terrorist Screening Database (TSDB). In the case of Abdulmutallab, although the FBI knew of his ties to Al Qaida and the State Department cable in which his father expressed concerns about his radicalization, these "dots" did not meet the FBI's criteria for his inclusion in the TSDB.[16] Inclusion in the TSDB would have required the FBI to have the information from TIDE, the CIA reporting and the State Department cable. In sum, there is incompatibility in the agencies criteria; NCTC, FBI, CIA, and the State Department; all have separate criteria for inputting someone on watch list such as TIDE and TSDB and intelligence databases. This dynamic complicates cross agency coordination.

Abdulmutallab's name was included in the NCTC's TIDE database, the CIA had knowledge of his AQAP affiliation, and the State Department did not correlate the concerns expressed in the Embassy cable with the fact that Abdulmutallab possessed a U.S. visa. In fact, a misspelling of his name led the State Department to believe that he did not have a valid visa. In hindsight, it is apparent that the "dots" were not connected but what is not apparent is who had THE "smoking dot" that would have allowed for the

fusion of data and ensured actions necessary to preempt the Christmas day attack? Even if the information was properly fused at the NCTC, it still may not have met the FBI's watch listing criteria. The combination of different watch listing criteria and the failure by the State Department to revoke Abdulmutallab's visa contributed to the decision to exclude him from the no fly list. In fairness, had the various agencies knew that their information was vital to preventing this attack, they would have taken the necessary actions to prevent the attack. However, to quote former Secretary of State Rumsfield "there are known knowns, known unknowns and then there are unknown unknowns".[17] This was a case of unknown unknowns as each element did not know they possessed a "dot" key to stopping this attack.

Analytical Priorities. Surprises such as 9-11, Fort Hood and Flight 253 cause policy makers to question analytical processes and seek foolproof methods and systems in a futile effort to totally eliminate surprise. The problem highlights a previously mentioned challenge for the IC; balancing the current priorities of national security policy makers with the requirement to provide strategic intelligence and warning. In the aftermath of surprises such as Flight 253, the tendency trends towards an increase in the amount of intelligence and criminal analytical effort focused on the development of systems that gather more information and create more stringent security requirements. The post 9-11 reform of the IC and the creation of DHS is the most extreme example of increasing systems, analyst and growth in government. These decisions indirectly impact the intelligence collection cycle and the analytical effort by changing analytical priorities.

Following the Christmas day incident, President Obama directed security upgrades to include tasking NCTC to set up a process for prioritizing and pursuing "thoroughly and exhaustively" terrorist threat threads, including follow-ups by intelligence, law enforcement and DHS authorities.[18] " Here, it is important to briefly highlight key differences in intelligence, law enforcement and their connection to DHS. Intelligence is the collection and analysis of information to produce intelligence that is used for pre-emptive action against a threat. Law enforcement is focused more towards the gathering of physical evidence to determine culpability in criminal acts. While there are preemptive law enforcement actions, their core competency is detective work in the prevention of criminal activity, not preemptive collection and analysis. Each technique creates hurdles in coordination and interoperability with regards to homeland security. By law, U.S. intelligence agencies cannot collect or store intelligence on U.S. persons and foreign intelligence pertaining to threats of a domestic nature must be shared with the FBI. Given the classification of intelligence data and collection sources, IC elements are sometimes reluctant to share information with the FBI. The prohibition of intelligence collection on U.S. persons, the FBI's criminal activity focus and as previously mentioned, different interagency cultures and priorities, are often an obstacle towards sharing intelligence that may preempt an attack on the homeland.

The President also directed other security upgrades to include "reviewing and updating the terrorist watch list system, adding more individuals to the "no fly" list, and directing our embassies and consulates to include current visa information in their warnings of individuals with terrorist or suspected terrorist ties."[19] While these measures seem prudent, the threshold for watch listing someone or what constitutes

threat reporting may become less stringent. Adding potentially thousands of names to various watch lists may strain analytical and collection resources due to database incompatibilities across the various agencies. The lack of compatibility forces analyst to "air gap" or manually enter names into databases to ensure compatibility. This manual process has a number of potential effects; it may create a backlog in updating watch lists; force a re-prioritization of where to assume analytical risks that someone not added to the list may be the next attacker or overload the collection system with potential false alarms.

The President also directed that the IC "begin assigning specific responsibility for investigating all leads on high-priority threats so that these leads are pursued and acted upon aggressively" and that intelligence reports, specifically those that indicate a potential threats to the United States, be distributed more rapidly and more widely.[20] The latter directive has implications on the tasking and allocation of national and theater level collection assets. This directive forces the reevaluation of current thresholds for analysis, production and dissemination of intelligence. Rapid analysis, production and dissemination of an ever increasing amount of information may not prove synonymous with quality analysis that leads to actionable intelligence. The unintended effect may be a larger volume of threat reporting that might distort the threshold for what constitutes a credible potential threat to the United States. The challenge for the intelligence leader is to work with decision makers at the appropriate levels to streamline analytical requirements and ensure timely dissemination of the most relevant intelligence. This process is more challenging at national level as the analytical effort tends to be

disconnected from policy makers and operational processes, making the production of relevant intelligence more challenging.[21]

Security Criteria. The recent events highlight issues in the U.S. air travel security apparatus. First, budget based U.S. airport security facilitates an inconsistent security baseline across the country. Additionally, TSA screening procedures and equipment span a wide range throughout the 50 states. Internationally, the screening of passengers is handled differently in each country ranging from threat criteria to how someone is searched to the type of screening equipment used. Further, TSA or affiliated private screening companies do not use U.S. terrorist databases for screening. Congressional law requires TSA to leave screening in the hands of the airlines. However, the airlines only have access to the "no fly" list, not terrorist databases.[22] In the case of Flight 253, Abdulmutallab flew from Lagos, Nigeria on a one way ticket with cash and no checked baggage. This did not raise a red flag for several reasons; incompatible communication between airlines, inadequate Nigerian screening procedures and different threat warning criteria between Lagos, Amsterdam and Detroit. Again, this was a potentially huge "smoking "dot" that was missing from the equation. The airline's lack of access to terrorist databases gave intelligence analysts a smaller window to gain insight of Abdulmutullab's travel plans on the front end of the flight versus finding out when he was enroute to the U.S. from Amsterdam.

Privacy. There is a dilemma between security and privacy. Policy makers are reluctant to implement security policies that might infringe on the privacy of citizens. These policies have a profound impact on the intelligence collection effort. By nature, there is a contradiction between intelligence and human rights. The nature of

intelligence collection infringes on human rights.[23] The bomb material concealed inside Abdulmutullab's underpants is detectable with the right type of equipment. However, sophisticated technologies that can find these bombs are expensive, time consuming, and not uniformly deployed at all international airports. The other alternative is to use simple procedures such as strip searches, employment of bomb sniffing dogs and secondary screening of suspicious passengers. The issue with this is again time, the encroachment on individual privacy and the potential for discrimination. Since 9/11, there have been numerous efforts by various organizations to stop invasive security procedures such as strip searches and secondary screening. Al Qaeda is likely aware of Americans sensitivity to infringement on privacy and they use this information as a means to exploit what they believe are security gaps in our system. This is likely the reason Abdulmutallab hid the material in his underwear and previously the "shoe bomber" Richard Reid hid material in his shoes. Al Qaeda elements assessed that an individual carrying explosives on his person would not be searched. Going forward, what will be the next tactic used in response to the screening and other security procedures implemented in the aftermath of the Flight 253? The next level of security measures must include a component that will not allow Al Qaeda to use our rights to privacy against us.

Bridging the Dots

The five commonalities outlined in the previous section provide a roadmap towards innovative methods of intelligence analysis that are weighted towards the current security environment. The three NIS mission objectives; combating extremism, provide strategic intelligence and warning and the integration of counterintelligence directly relate to recent incidents. Going forward, the key to staying ahead of potential

threats and providing actionable intelligence that facilitates “connecting the dots” may hinge on our ability to discern changing extremist tactics, the balancing of current and long term intelligence analysis to guard against strategic surprise and the effective integration of counterintelligence (CI).

Combating Extremism. Extremism is defined as religious radicalism as exercised by various terrorist groups such as the Al Qaida factions. These groups use their ideology to justify attacks on U.S. citizens and interest. In the combating of extremism, there must be an understanding of shifting extremist strategies from recruitment practices to operative training. Understanding this threat may require a combined interagency task force to examine trends for extremist modus operandi. Further, we must understand how shifting extremist strategies affect operative competence, indoctrinization techniques and emerging operational strategies to counter U.S. security and intelligence practices. Using the example of Flight 253, the timeline depicting Abdulmutullab’s training for the Christmas day incident represents a period of around 90 days from approximately September when he traveled to Yemen to the Christmas day incident.[24] The question for the IC is to understand if this apparent quick attack preparation represents a shift in Al Qaida’s strategy for training, indoctrination and mobilization for attacks. Understanding these types of indicators and having the cognitive agility to adjust analytical priorities are a prelude towards “connecting the dots”; allowing for Indications and Warning (I&W) measures, the cueing of assets and cross agency coordination.

Provide Strategic Intelligence and Warning: The nature of current threats and policymaker predominance with current intelligence creates challenges in applying

strategic intelligence practices. Given the increase in threat actors and the effects of information overload and globalization on the security environment, the demand for strategic intelligence and warning capability supporting actionable intelligence will likely increase in the next 5 years.[25] Translated, this requires rapid increases in our proficiency towards finding the "smoking dot". Strategic intelligence and warning strategies must adhere to some basic principles to address this fluid environment. These principles have been either advocated or used previously within the IC. First, strategic intelligence leaders must understand that a component of successful analysis is the framing of the operational environment. Framing provides a mechanism to project emerging threats and the scope of an adversary's capability.[26]

Next, to help break interagency bureaucracy, intelligence products should follow the intelligence "pyramid" advocated by CIA analyst Sherman Kent, who served from 1950-1967. Kent's "pyramid" concept advocated a close relationship between analyst and their policy counterparts. Kent believed that products resulting from intelligence research and surveys must be fully disseminated to a wide spectrum of intelligence officials in the desk officer level of policy agencies and departments and tailored for dissemination to officials at various levels of government.[27] Additionally, due to the interrelation of the various instruments of power, these products should also be disseminated to other agencies or departments such as Energy, the Drug Enforcement Agency (DEA) and Treasury to name a few. These agencies can add additional insights and allow for analysts to see missing dots or identify critical new ones. The resulting whole of government strategic surveys should not only enable strategic warning but also stimulate collaboration and increase expertise.

Integrate Counterintelligence (CI): In the Afghanistan theater, the lack of relevant intelligence and the December 2009 deaths of 7 CIA analysts at the hand of a Jordanian double agent magnify the importance of counterintelligence in validating intelligence sources, understanding foreign cultures and penetrating and exploiting adversaries.[28] Forward deployed CI is necessary to maintain a global intelligence infrastructure that provides surge capability and warning in the case of an emerging international threat.

In a globalized world, non-state actors potentially pose a greater CI threat than nation states. Further, there is a synergy between terrorism, drugs, crime and rogue nation states. More threats mean more potential "smoking dots" emanating from a wide array of potentially interconnected threats. Transnational organizations may attempt to gather U.S. intelligence and exploit it among themselves to further their respective interest. CI facilitates linkages that allows for the discernment of relations between nefarious actors, their intentions and the impact of their actions on U.S. interest. The integration of CI mandates a paradox in which the CI analyst may have to penetrate and compromise friendly networks.[29] Unlike nation states, extremist groups and non-state actors do not have robust intelligence apparatus. In fact, they can use OSINT to gather information about our intelligence efforts against them and remain under the radar by hiding within the "fog" of information. CI ability to protect critical information, identify threat actors seeking such information and the ability to provide early warning is key to prevention of strategic surprise and pre-empting the "smoking dot".

Finally, apart from having the cognitive agility to adjust to a constantly changing security environment, the IC must use enabling technologies that diminish the fog of

uncertainty caused by information overload. These technologies must be interoperable, accepted and understood by citizens and provides additional security that is enduring and does not infringe on our civil liberties. Biometrics is a capability that will provide another IW layer by identifying nefarious actors, mitigating strategic surprise and enhancing CI efforts to facilitate our ability to find the "smoking dot."

Biometric Analysis: Managing Uncertainty by Illuminating the Threat

Biometrics is a subset of Forensics Science that measures an individual's physical or behavioral characteristics and uses these characteristics to identify a subject.[30] BEI is also classified as Identity Intelligence (I2); information derived from an individual's distinct physical or behavioral data that is analyzed with other elements of intelligence to attain the identity of an adversary.[31] Identity formulation is based on three factors of authentication: something you know such as passwords or pin numbers, something you physically have such as a driver's license or passport and something you are which includes your unique physiological and behavioral features.[32] Biometric data includes 7 primary modalities with retinal and iris scans, fingerprinting and facial recognition being the most prominently used. The other modalities are DNA samples, and behavioral actions such as speech patterns and gait analysis. DNA sampling and fingerprinting are prominent techniques used in the law enforcement world in the analysis of crime scenes and attaining attribution of criminals.

The evolution of biometrics coincided somewhat with the proliferation of information systems. Items such as military CAC cards, smart cards or credit cards with magnetic strips and airport retinal scanning are forms of biometrics; all designed to ascertain the identity of an individual. Biometric matching entails the confirmation of someone's identity using two or more pieces of biometric data that may have been

collected in different locations. Biometric matching can also be used in association with other forms of intelligence to discern possible intent or participation in past incidents. Terrorist and criminals seek to protect their identities through identity deception techniques such as the use of aliases, fake passports, or driver's licenses. However, fingerprints do not change nor do other forms of Biometrics.

Post 9-11, the use of biometrics is more prominent in the war on terrorism and has proven its value in both Afghanistan and Iraq. In Afghanistan, the Marines are using fingerprint devices, iris scanners and electronic databases to screen local residents applying for jobs requiring security clearances; additionally, in Iraq, there are over 1,000 Biometric Automated Toolsets (BAT) employed. BAT is a laptop based computer system which collects and stores biometric data. There have been numerous success stories, specifically in Iraq. In 2004, Marines used biometric collection devices to secure the city of Fallujah. After heavy fighting, the Marines closed the city off leaving a limited number of entry and exit check points. Over 250,000 retinal and fingerprint scans were collected on the citizens of Fallujah. [33] As citizens exited and re-entered the city, their biometric data was checked against BAT. The biometric collection led to a dramatic reduction in violence due to the inability of Sunni insurgent and Al Qaida elements to access the city for fear of compromise of their identity. The second and third order effects were an increase in U.S. force credibility with the populace which enabled better intelligence through information received from a secure populace.

In December 2004 at the U.S. Base near Mosul, a suicide bombing killed 22 people and injured 72. An investigation of the attack revealed that the facility's badging

system was “exploitable”. The facility needed an improved system for base access security that better identified the enemy as they attempted to enter.[34] The Biometric Identifications System for Access (BISA) was developed. Since its development, BISA has been used by analysts to issue more than 220,000 military base access smart cards and permanently bar more than 800 individuals from accessing to U.S. facilities in Iraq. The result is a force protection asset that increased base and checkpoint security with the use of Biometrics-enabled badges and employee screenings.[35]

These theater success stories contributed to a national emphasis on the creation of an enduring biometric capability. In June 2008, President Bush issued Homeland Security Presidential Directive (HSPD) 24. This directive mandates the establishment of a framework for the collection, storage and sharing of biometric data on known and suspected terrorist (KST) while respecting the privacy and legal rights of individuals.[36] In January 2010, the House of Representatives Resolution 2647 called for increases in the Science and Technology development of BEI to fight transnational threats.[37]

There are isolated success stories of biometric data sharing partnerships between DoD and DHS elements such as the National Ground Intelligence Center (NGIC) and the U.S. Coast Guard’s National Maritime Intelligence Center’s (NMIC) biometric data sharing agreement. As part of it’s DHS mission, the NMIC facilitates biometric data exchange through interface with the El Paso Intelligence Center (EPIC), a fusion center containing intelligence analyst from each of the 22 DHS agencies. Although limited, this is an effort towards coordination between intelligence and law enforcement entities. Other initiatives include DHS and intelligence elements integration of the biometric data of terrorist encountered in Iraq and Afghanistan into

current watch list and ongoing efforts to develop biometric data sharing agreements with other countries.[38]

The primary challenges facing the U.S. biometrics community include interoperability gaps, adherence to biometric standards, lack of clear government policy, and privacy concerns.[39] As previously mentioned, there is great demand for advanced biometric solutions by the White House, DoD, and DHS through initiatives such as HSPD 24 and HR 2647. The private sector is trying to play catch up to the government demand. However, more advancement in multi-modal equipment and continued emphasis on research and development is needed to improve data collection, accuracy and system interoperability.

Many of the DoD and Homeland Security databases that contain biometric data are not integrated or are incompatible. Much of the biometric data must be "air gapped" or manually uploaded into biometric databases. The National Ground Intelligence Center (NGIC) maintains DoD's most extensive biometric data repository, the Automated Biometric Identification System (ABIS). Currently, they are working with a number of DoD and interagency elements to assist them in uploading biometic data into their watch list. Although the process is improving, there are still interoperability issues between different agencies such as legacy databases and stovepiped processes.

These issues combined with the vast amount of information available causes backlogs in data input. One example is NGIC's collaboration with NCTC to upload biometric files into the TIDE database.[40] NCTC's criteria for entry into TIDE is for known suspected terrorist (KST) while the NGIC criteria for ABIS entry includes combatants from Iraq or Afghanistan that may not necessarily be classified as a KST. In attempting

to upload biometric data from the NGIC, the names of KST individuals must be manually inputted into TIDE. The FBI contains the world's most extensive database of fingerprint information with approximately 50 million templates in its master file. Yet, the process of obtaining a match is cumbersome and the FBI's fingerprint databases do not fully interact with biometric databases within DHS and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT).[41] Various U.S. government institutions have developed other biometric systems such as TSA Fly Clear and ABIS. The US-VISIT program is deployed at over 100 airports around the world to collect fingerprint data as part of a visa application for anyone wishing to visit the U.S. Once their biometric data is collected, it is checked against US-VISIT for known criminals and suspected terrorist. The data is then used to validate the person's identity upon arrival at a U.S. airport.[42] Although US-VISIT checks the biometric data, the database is not compatible with other DoD or DHS databases. Therefore, a terrorist enrolled in ABIS or TIDE overseas could still obtain entry into the US because the US-VISIT database would not have visibility of the information available from the other two government agencies. Thus was the issue of Flight 253. Abdulmutullab was in the NCTC's TIDE database but still was able to obtain a visa. Database compatibility between TIDE and US VISIT would have possibly enabled a biometric match toward "connecting the dots". Again, another key "dot" was missed by not having his biometric data in US VISIT.

Integration of a national biometric system must include interoperability of the internal databases and policies of the FBI, DoD, DHS and TSA. Effective cross government integration of this capability denies terrorist and other non-state actors what they most covet, the maintenance of their anonymity. Nationally integrated biometrics

provides another layer of defense and serves as an Indications and Warning (I&W) mechanism. Through a nationally integrated biometric system, U.S. authorities will have the tools to determine a person's previously used identities and track past activities; particularly as they relate to terrorism and criminal acts while there is still time to thwart an attack. Further, a biometrics match on an individual detained at an airport or by U.S. military or Border Control sends a red flag regarding the intentions of the individual, allowing for the possible pre-emption of a hostile act. In addition to linking a person quickly to his or her previously used identities, biometrics helps authorities determine if a person they encounter has been previously arrested in the United States or other countries, been refused entry into the United States, or is somehow linked to terrorist or criminal activity.

How do we improve the quality of our intelligence analytical effort , processing and security without infringing upon the rights of American citizens? First, there is a need to be more open about some of our intelligence gathering methods. Much of intelligence collection comes from open source data. Legislation was put in place in the 1990s to ensure that information collected on U.S. persons by the state for one purpose could not be used for another. Since 9/11, this policy has largely been ignored as data warehouses were put in place to manage the vast amount of information.[43] This evolution of data warehouses indicates there is a threshold for intelligence gathering and minimal intrusion on privacy, specifically in the aftermath of an attack. Here is an opportunity to implement additional intelligence gathering measures that are clearly defined, ethical and non-coercive.

The creation of a national biometric system passes the feasibility, acceptability and suitability (FAS) test. The policy is feasible based on U.S. technological advantages, economic viability through consolidation of capability versus development of costly organizationally focused biometric systems. It is acceptable based on its importance to national interest and adherence to enacted policies ensuring the rights of U.S. citizens. Finally, the policy is suitable based on the desired end of improving our ability to advance U.S. security infrastructure and guarantee better security for the American people.

Conclusion

The evolution of information systems and technology complicates the current security environment. Intelligence professionals operate in an increasingly uncertain and complex environment characterized by a proliferation of undefined hostile state and non state actors. The strategic uncertainty muddies the nation's threat assessment by painting extremist groups like al Qaeda as both trans-national "national security threats" and as groups of terrorist criminals who could be "brought to justice."[44] Combating transnational threats that dilute the lines between international and domestic security or terrorist vs. criminal requires clearly articulated and focused policies that enhance intelligence but does not infringe on civil liberties.

Intelligence officials must balance demands for national intelligence systems to collect more data while ensuring the most relevant information is processed and analyzed for intelligence production. Policy decisions impact intelligence analytical priorities and add to an uncertain threat environment. Recent U.S. policy facilitating documents like the NIS, HSPD-24 and HR 2647 represent a paradigm shift in addressing 21st century threats by highlights ends and ways to address the ever

changing threat environment. The implication for the IC is clear: develop innovative ways to further intelligence gathering efforts as community reform efforts continue.

Recent incidents highlight the necessity to further consolidate, innovate and constantly reassess our national intelligence collection and analytical priorities. We must do this in a threat environment characterized by threat actors willing to use a variety of tactics and techniques to attack America. As incidents over the past 90 days imply, technology and information, while valuable; contribute to an uncertain threat environment. As technology and information proliferates, the probability of strategic surprise proliferates.

Improving security and diminishing uncertainty requires policies for better interoperability of intelligence and interagency databases and utilizing enabling technology such as Biometrics through implementation of a national level biometrics program. A national Biometric program is an innovative means towards disrupting transnational threats and illuminating hostile actors Biometrics is an enduring technology that if effectively integrated will enhance U.S. security, improve collaboration between domestic and foreign intelligence and enhance interoperability between DoD, DHS, State Department and the FBI.

The three highlighted NIS objectives; combating extremism, provide strategic intelligence and warning and integrate CI are directly relevant to the events of the past 90 days and post incident intelligence scrutiny. These objectives illustrate 3 underlying IC imperatives; balancing current priorities of national security policy makers, minimizing strategic surprise and overcoming bureaucratic cultures that impede good collaboration while maintaining the competencies of various collection agencies.

Intelligence focused on a myriad of transnational and homeland security threats must be a coordinated whole of government effort. Failure cannot stem from an inability to disseminate known information, agency bureaucracy or system incompatibility. To effectively identify and overcome information gaps, there must be an appreciation of agency priorities, and targeting procedures.

There is no "silver bullet" to screening procedures, intelligence gathering methods, technology and spending that will ensure a 100% success rate. Getting closer to a 100% success rate will require more than simply increasing collection and analysts. It will require a whole of government approach that uses a combination of technologies and policies reinforced by the intelligence effort to "connecting the dots."

Endnotes

[1] Dennis M. Murphy, *"Strategic Communication: Wielding the Information Element of Power,"in* U.S. Army War College Guide to National Security Issues, Vol. 1: The Theory of War and Strategy, ed. J. Boone Bartholomees, Jr., (3rd edition). Carlisle Barracks, PA: Strategic Studies Institute, 2008. Chapter 12, pp. 175-176.

[2] MG Michael Flynn, Captain Matt Pottinger and Paul Batchelor, *Fixing Intelligence: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, D.C.: Center for a New American Security, January 2010), 4.

[3] The President of the United States, Barack Obama, Remarks by the President on strengthening Intelligence and Aviation Security, Washington, DC, January 7, 2010.

[4] Jennifer E. Sims and Burton Gerber, eds., *Transforming U.S. Intelligence*, (Georgetown University Press, Washington, DC, 2007), pp ix-xiii. Other challenges mentioned are the issues of interoperability, clandestine collection, availability of overseas intelligence facilities and meeting the needs of tactical operators.

[5] The National Intelligence Strategy of the United States of America, August 2009. The other 3 are counter WMD proliferation, enhance cybersecurity and support current operations.

[6] LTC(P) Rick Emerson. In my most recent assignment, I served as the Intelligence and Security Command's Biometric Division Chief. I was also exposed to this capability while assigned to Multi-national Forces Iraq in 2005. In my capacity as the Chief of Current Intelligence, I frequently interacted and received reporting from the Combined Explosives Cell (CEXC) which handled forensic materials selected in the aftermath of attacks.

[7] James J. Carafano Ph.D., *Re-learning the Lessons from the thwarted Detroit Airline Bombing,* The Heritage Foundation (December 28, 2009), 2.

[8] Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack, pp. 2-3.

[9] Douglas MacEachin, "Analysis and Estimates", *Transforming U.S. Intelligence,* eds. Jennifer E. Sims and Burton Gerber, 116.

[10] General Michael Hayden, interview with Voice of America, Global Security.org, January 5, 2010.

[11] Peter Gill, *Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'*, Intelligence and National Security, Volume 22 (February 2007), 79-82.

[12] Christopher Drew, *Drone Flights Leave Military Awash In Data*, New York Times, JAN 11, 2010.

[13] 50 U.S.C. & 404o(d)(1).

[14] 50 U.S.C.& 403-4a(d)(2).

[15] Summary of the White House Review of the December 25, 2009 Attempted Terrorist Attack, 3.

[16] Ibid, 5.

[17] Donald Rumsfeld, Defense Department briefing, 12 February 2002, http://www.globalsecurity.org/military/library/news/2002/02/mil-020212-usia01.htm4 (accessed 18 JAN 2010)

[18] Reuters report, *Factbox: Actions Obama ordered after December 25 bomb plot*, (7 JAN 2010).

[19] Remarks by the President on Strengthening Intelligence and Aviation Security, 7 JAN, 2010.

[20] Ibid.

[21] William E. Odom, *Intelligence Analysis,* Intelligence and National Security, Volume 23 (June 2008), 320-325. The author argues that where the analyst is located has an impact on the quality of their analysis. If analyst are separated from the planning and operational processes and are not in daily contact with operational staffs, how are they to know, in a timely fashion, what analysis is needed or relevant? They will not have an understanding of false assumptions about adversaries that underpin plans and operations and they have less ability to inform planners of flawed concepts.

[22] Carafano, 2.

[23] M. Quinlan, '*Just Intelligence: Prologomena to an Ethical Theory*', Intelligence and National Security 22/1 (2007), 2.

[24] Various reports indicated that when Abdulmutullab's father went to the American embassy in November 2009, he reported on his son's plans to travel to Yemen. The key information regarding the attack was gathered between October and December.

[25] Jennifer E. Sims, *Transforming U.S. Intelligence,* 25-26*.*

[26] LTG Richard Zahner, *"Threat Update"* briefing slides with scripted commentary, Carlisle Barracks, PA, U.S. Army War College, October 14, 2009.

[27] Sherman Kent, *"Estimates and Influences," in Sherman Kent and the Board of National Estimates: Collected Essays,* ed. Donald Steury (Washington, D.C.: CIA Center for the Study of Intelligence, 1994)*, 33-42.*

[28] MG Flynn, *Fixing Intelligence,*7-8. The study concludes that the IC needs to shift focus from the focusing on collection against insurgent groups to learning more about the environment by gathering information on the political, economic and cultural environments.

[29] Sims, *Transforming U.S. Intelligence,* 21-23*.*

[30] Colonel Eloy Campos, *Consolidating our Country's Biometric Resources and the Possible Implications,* US Army War College Strategic Research Project, 15 March 2008, 1.

[31] Emerson.

[32] Report of the Defense Science Board Task Force on Defense Biometrics (Washington, D.C.: Office of the Undersecretary of Defense, March 2007).

[33] Campos, 2.

[34] Jeff Erlichman, *Telling friend from Foe,* Washington Technology, FEB 2010.

[35] "Biometrics on the Ground and in DoD", Soldier Magazine, Volume 65, No. 2 (FEB 2010)

[36] Homeland Security Presidential Directive 24, June 5, 2008. The directive establishes a framework to ensure that Federal executive departments and agencies use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting information privacy and other legal rights under United States law.

[37] National Defense Authorization Act , H.R.2647: FY 2010. The bill directs DOD to report on its progress in developing a framework for operational and strategic analysis of biometrics-enabled intelligence. The committee is concerned DOD is not maximizing the benefits of this type of intelligence to fight threats that transcend geographic boundaries.

[38] Emerson. This was being discussed at the Pentagon by various biometric steering committee and working groups.

[39] Ms. Martha Karlovic and Mr. Thomas Giboney, *Strategies for Implementing HSPD-24,* National Defense Industrial Association, opening remarks 2009 Biometrics Conference.

[40] Emerson. In my capacity as INSCOM Biometric Division Chief, this was one of the initiatives to share biometric data.

[41] Campos, 5. remarks 2009 Biometrics Conference.

[42] U.S. Department of the Army, *Biometrics Task Force, DoD ABIS*, Trifold.

[43] Peter Gill, *Security Intelligence and Human Rights*, 84.

[44] Goss, DOD Challenges in HLD / HLS 1 Homeland Security Affairs, (http://www.hsaj.org), 2006.